Forum of European Supervisory Authorities for Electronic Signatures (FESA)

Public Statement on Server Based Signature Services

October 17, 2005

In the course of the last few years, a new architecture of electronic signatures services has emerged: Server based signature services. The main idea is that the signature creation data are not stored in a signature creation device located at the signatory, but in a central hardware security module located at the signature service provider. In order to create an electronic signature, authentication data and data to be signed or a hash of data to be signed are sent from the signatory to the provider via a secure communication channel. After verification of the authentication data, the signature is created by the hardware security module, and signed data are returned to the signatory for further processing.

This paper presents the common understanding of FESA members with respect to using server based signature services for creating advanced or qualified electronic signatures[1]. Directive 1999/93/EC contains two requirements which are relevant to server based signature services:

- The definition in Article 2 of the Directive requires that an advanced electronic signature *is created using means that the signatory can maintain under his sole control*.
- According to Annex III of the Directive, secure signature-creation devices must, by appropriate technical and procedural means, ensure that *the signature-creation data used for signature generation can be reliably protected by the legitimate signatory against the use of others*.

Sole control

The meaning of "sole control" in Article 2 of the Directive has been discussed in the FESA working paper on advanced electronic signatures (http://www.fesa.rtr.at/public-documents/WorkingPaper-AdvancedSignature-20041012.pdf). According to that paper, the use of special hardware as signature creation device is not required. However, the signatory must take measures to maintain control over his key. The security concept and the system configuration of the server must ensure that only the signatory, who is either a natural or a legal person, has control over the corresponding signature creation data.

If signatures are created automatically at a server, the signatory is usually not present in person. However, the signatory has control over security measures, and has the responsibility to select suitable security measures.

For server based signature services, the signatory is not present in person either. But neither can he select suitable security measures. He can only choose whether or not to enlist the services. The signatory can decide whether or not security measures taken by the service provider are sufficient for him. For making this decision, the signatory needs at least

- access to a comprehensible version of the security concept and
- confidence that the service provider sticks to the security concept (confidence can be strengthened by audits performed by a trusted third party like an independent auditor or a supervisory authority).

In addition, sole control requires certain cryptographic qualities of algorithms and of signature creation data that have been discussed in the working paper mentioned above.

[1] The term "qualified electronic signatures" is used for advanced electronic signatures which are based on a qualified certificate and which are created by a secure signature creation device.

Under these premises, FESA members believe that sole control at least of the signature creation data can be achieved and that advanced electronic signatures can be created by a server based signature service[2].

Reliable protection by the legitimate signatory

Reliable protection of signature creation data implies that some sufficiently strong authentication mechanism keeps the signature creation data from being used by others. Authentication data have to be protected all the way from the human interface to the server. The provider must not store authentication data in a way that allows abuse by its personnel or by third parties. Moreover, the data to be signed must not be altered before signature creation. All communication between the signatory and the server has to be performed over trusted channels.

The Common Criteria protection profile for secure signature creation devices (CWA 14169) requires a trusted path for user authentication if the human interface is not provided by the target of evaluation. It also requires a trusted channel between the signature creation application and the secure signature creation device. Fulfilment of these requirements can only be assessed by evaluating the whole system, including communication between the signatory and the signature creation device. This task seems by far more complex than evaluation of a smartcard.

Although there is no obligation to follow a generally recognised standard like CWA 14169, if the conformity of a SSCD is assessed by a designated body according to Article 3(4) of the Directive, such a body must comply with Commission Decision 2000/709/EC. According to this Decision, a designated body must be transparent in its conformity assessment practices and is liable for its activities. Because of these regulations, most designated bodies require successful evaluation and certification of secure signature creation devices as a prerequisite of conformity assessment. As of October 17, 2005, no server based signature service has been evaluated as a secure signature creation device.

Apart from Germany, where the services in question cannot be used in this context at all, FESA members cannot rule out that server based signature services could be used for creating qualified electronic signatures. At present, however, this seems to be rather unlikely.

[2] Note that according to German law, “sole control” implies physical control and that therefore in Germany, server based signature services cannot be used for creating advanced electronic signatures and definitely not for creating qualified electronic signatures.